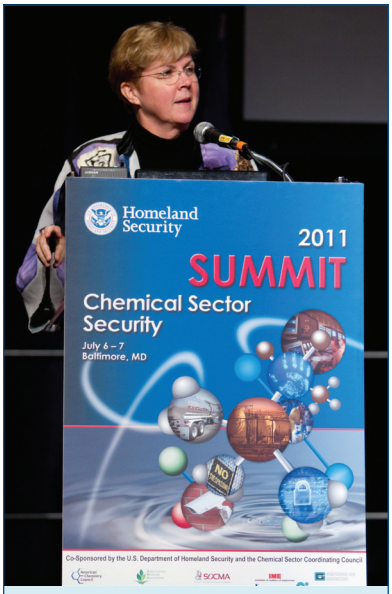
Homeland Security

NIPP NEWS

IN SUPPORT OF THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

ISSUE 62: JULY - AUGUST 2011

Fifth Annual Chemical Sector Security Summit Highlights Progress in Voluntary and Regulatory Programs



Deputy Secretary Lute addressing the Summit

More than 500 Department of Homeland Security (DHS) partners from around the country gathered in Baltimore in July for the fifth annual Chemical Sector Security Summit. The Summit is an annual forum for DHS and its partners in the private sector to share information, highlight best practices, and discuss ways to enhance collaboration in order to build a safer and more resilient homeland.

DHS Deputy Secretary Jane Holl Lute presented the keynote address, thanking the Chemical Sector Coordinating Council for co-sponsoring the Summit and commending the chemical industry for its efforts to enhance security. Deputy Secretary Lute also highlighted some of the progress made during the past decade, and stressed the importance of government and industry working together to better understand the risk landscape. She encouraged continued and increased information sharing, saying, "Chemical Sector partners seek clarity, predictability, and a level playing field. You want to be engaged, you want to know more about threats—so do we; you want to reduce your vulnerabilities—so do we."

Assistant Secretary for Infrastructure Protection (IP) Todd Keil reflected on the evolution of the Summit over the past five years. He cited the steady growth of attendance and noted that "the Summit reflects a true partnership at work, where public and private sector representatives share information and develop tools necessary for our industry partners to enhance their security posture." He reiterated the Department's commitment to implementing and enhancing both voluntary programs and the Chemical Facility Anti-Terrorism Standards (CFATS). Assistant Secretary Keil also announced the new leadership team for the Infrastructure Security Compliance Division, which oversees CFATS—Director Penny Anderson and Deputy Director David Wulf.

The 2011 Chemical Sector Security Summit featured a wide array of session topics including DHS voluntary programs and resources, the CFATS and Ammonium Nitrate regulatory programs, theft and diversion threats, global supply chain security, suspicious activity reporting, and personnel surety, to name a few. In addition to the two-day Summit, this year's event included two days of resource demonstrations and workshops.

To view presentations from this year's Summit, please visit the Chemical Sector Security Summit Web site at www.dhs.gov/chemicalsecuritysummit. For more information on the Summit, contact Amy Graydon at ChemicalSector@dhs.gov.

Topics in this Issue

DHS Launches Cyber Risk Management Methodology

Threats against the Nation's cyber infrastructure have increased both in sophistication and in frequency in the past few years as hackers, cyber criminals, terrorists, and sophisticated state and non-state actors seek to exploit vulnerabilities for financial gain, criminal activity, intelligence gathering, and propaganda.

The DHS National Cyber Security Division (NCSD) has launched its Cybersecurity Assessment and Risk Management Approach (CARMA) to assist critical infrastructure sectors; State, local, tribal, and territorial governments; and other public and private sector partners in their efforts to assess and manage cyber infrastructure risk.

CARMA provides a picture of sector-wide risks for different categories of cyber critical infrastructure, allowing sectors to prioritize their cyber risks at a strategic level. It is a flexible, scalable, and reusable cyber risk management approach that incorporates lessons learned from a wide variety of cybersecurity activities, including recent successes within the Information Technology Sector in identifying and addressing cyber risk.

CARMA provides critical infrastructure owners and operators, as well as key public and private sector leaders and decision makers, with several distinct benefits:

- Clarifies the role of cyber critical infrastructure in supporting critical missions and functions, to help in identifying cyber dependencies and interdependencies across functions, as well as potential cascading effects;
- Prioritizes national-level cyber risks, to provide a roadmap for sector cyber risk management activities and reporting; and
- Complements asset and facility-based security assessments and operational risk activities by providing strategic cyber risk context to vulnerability and site assessments as well as cyber incidents.

Since development of the methodology, NCSD has discussed CARMA with a majority of the critical infrastructure sectors and subsectors, several State and local entities, and a number of internal DHS components. NCSD plans to conduct assessments with relevant stakeholders within the next year.

For more information on the CARMA process and how it could be scaled or piloted to support your sector in identifying, analyzing, prioritizing, and addressing cyber risks, please contact NCSD_CIP-CS@dhs.gov.

IP Continues Stakeholder Dialogue Aimed at Increasing Infrastructure Protection and Resilience

As part of its ongoing commitment to enhance security and resilience through strengthened partnerships, the DHS National Protection and Programs Directorate's Office of Infrastructure Protection (IP) continues to solicit stakeholder input in identifying the tools needed to effectively manage risks to the Nation's critical infrastructure. In late August, IP hosted two focus group discussions with critical infrastructure owners and operators to discuss the approaches they are taking to advance security and business continuity and the extent to which their activities are appropriately supported by IP programs and tools. The findings from these sessions will inform IP's effort to more closely tailor its voluntary programs to the requirements of its partners in the private and public sectors.

In the spring, IP and The Conference Board jointly hosted three regional workshops on resilience to enable senior executive-level security and business continuity officers to share their company's approach to resilience and the extent to which that approach is dependent on cross-sector and government engagement.

The Conference Board facilitated the workshops, held in Pittsburgh, PA; Raleigh, NC; and St. Louis, MO. Each region's DHS Protective Security Advisor arranged for owners and operators to attend the forum and offered their perspective on infrastructure resilience efforts. Four central observations were identified by all three forums:

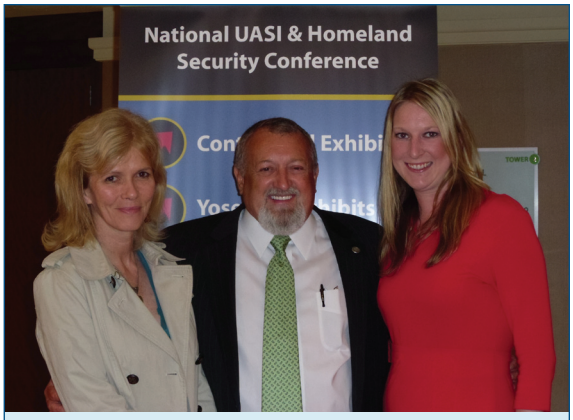
- Infrastructure resilience is rooted in integrating and enhancing risk analysis, business continuity, crisis management, and employee readiness.
- A company is only as resilient as its level of engagement in understanding and addressing—through external partnerships—its dependencies and interdependencies.
- Although owners and operators are primarily responsible for their company's resilience posture, government is needed to help restore critical sector functions and provide accurate risk and incident information.
- Infrastructure resilience requires greater executive support and resources.

These four findings provide IP and its mission partners with valuable insight into how the private sector is approaching and operationalizing infrastructure resilience. The findings were consistent with those found in a recent report on infrastructure resilience by the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). Both the workshops and the SLTTGCC report emphasize the central role played by public-private partnerships and the importance of understanding sector dependencies and interdependencies to advancing a region's resilience posture.

The Conference Board will complete a full report on the workshops this fall. For more information, please contact Sector.Partnership@dhs.gov.

UASI Conference Spotlights Critical Infrastructure Partnerships and Effective Information Sharing

For the third year in a row, IP co-organized the Critical Infrastructure Public-Private Partnership track at the National Urban Areas Security Initiative (UASI) and Homeland Security Conference, which was held this summer in San Francisco, CA. Titled "Enhancing Capabilities through Regional Collaboration," the conference provided an opportunity for over 1,500 public and private sector stakeholders to share information about ongoing efforts to secure the Nation and its larger urban areas.



Panelists from the Cross-Sector Regional Public-Private Partnerships session include (left to right)

Cherrie Black, New Jersey Office of Homeland Security, SLTTGCC Chair, SLTTGCC Regional Partnership Working Group (RPWG) Chair; Mike McAllister, Deputy Secretary of Virginia Veterans Affairs and Homeland Security, SLTTGCC RPWG Member; Kelly Barcic, Pittsburgh Regional Business Coalition for Homeland Security

Speakers included representatives of existing public-private partnerships; government, industry, and academic leaders in critical infrastructure protection; IP personnel, including Protective Security Advisors; and the FEMA Private Sector Division. The sessions allowed participants to openly discuss challenges and effective practices in the areas of building and sustaining sector-specific and cross-sector partnerships, incorporating the private sector into emergency operations and suspicious activity reporting, and protecting private sector information.

Some of the overall challenges participants identified include:

- Identifying resources to maintain partnership operations;
- Setting partnership expectations, priorities, and focus;
- Establishing mechanisms to support real-time situational awareness;
- Practicing robust collaboration to respond to emergencies; and
- Ensuring the protection of shared information.

Participants also identified several effective practices, both in partnership development and information sharing. These included:

- Ensuring the most appropriate sectors and disciplines are represented in partnership deliberations and activities;
- Continuously demonstrating value to participants by sponsoring critical infrastructure activities;
- Creating linkages in information sharing by enacting appropriate policies and procedures;
- Leveraging mechanisms to gather and disseminate information;
- Engaging the general public and private sector partners; and
- Ensuring the protection of data submitted to the government.

The conference provided robust discussions of the challenges and opportunities faced by infrastructure owners and operators in or near urban areas, and served as an example of the importance of communication and collaboration during both steady-state and incident response conditions. For more information on the UASI conference, contact Sector.Partnership@dhs.gov.

Resilient Constellation Exercise Series Focuses on Critical Infrastructure Owners and Operators

IP is sponsoring a new exercise series focused on information-sharing activities during threat, incident, and post-incident phases—the Resilient Constellation Exercise Series (RCES). The exercise is similar to the broader National Level Exercise (NLE) conducted each year, but with a primary focus on critical infrastructure owners and operators. As the threat environment continues to evolve, so too does the role of the Nation's critical infrastructure owners and operators.

RCES will engage critical infrastructure owners and operators; Federal Government stakeholders; State, local, tribal, and territorial governments; and other relevant partners, providing them with the opportunity to assess internal security measures and share information with other critical infrastructure stakeholders. The exercise consists of a series of events, including national, regional, and facility-level discussion-based exercises, operations-based exercises (to include limited full-scale play), and a post-event after action workshop.

The draft objectives of the RCES are:

- Evaluate multidirectional information management and sharing among select portions of the homeland security enterprise during a period of heightened awareness in accordance with applicable plans and procedures.
- Evaluate multidirectional information management and sharing among select portions of the homeland security enterprise following domestic attacks on critical infrastructure and a continued threat in accordance with applicable plans and procedures.
- Assess the effectiveness of protective measures implemented by select portions of the homeland security enterprise in accordance with applicable plans and procedures in order to enhance critical infrastructure protection and resilience to potential attacks.
- Assess impacts to industry of protective measure implementation based on the perceived threat, response, and National Terrorism Advisory System changes.

The RCES began with the Concept and Objectives meeting on August 5, 2011, and will run until the After Action Conference planned for February 2013. For more information, contact RCES@hq.dhs.gov.

> Resources Available for DHS Critical Infrastructure Partners

Infrastructure Protection (IP) sponsors a free online NIPP training course at http://training.fema.gov/EMIWeb/IS/crslist.asp. IP also has a trade show booth available for sector use. Please contact NIPP@dhs.gov for information on IP participation and/or exhibition at an upcoming sector event or to schedule a trained speaker for your event.

> Implementation Success Stories

IP continues to seek NIPP and/or SSP implementation success stories from the sectors to be shared with other critical infrastructure partners. Please submit suggestions or brief write-ups to NIPP@dhs.gov.

> NIPP News

NIPP News is produced by the Office of Infrastructure Protection. NIPP partners are welcome to submit input. To submit information for inclusion in upcoming issues, please contact NIPP@dhs.gov. Recipients of this newsletter are encouraged to disseminate it further to their critical infrastructure partners.

> Learn more about the DHS critical infrastructure protection program at www.dhs.gov/criticalinfrastructure.